COMMONWEALTH OF VIRGINIA

Information Technology Resource Management Guideline

INFORMATION TECHNOLOGY SECURITY GUIDELINE

Department of Technology Planning

Preface

Publication Designation

COV ITRM Guideline SEC2001-01.1

Subject

Information Technology Security

Effective Date

December 7, 2001

Supersedes

No prior security guidelines

Scheduled Review

One (1) year from effective date

Authority

Code of Virginia § 2.2-226
(Powers and Duties of the Secretary of Technology)

Code of Virginia § 2.2-2651
(Powers and Duties of the Council on Technology Services)

Code of Virginia § 2.2-1701
(Powers and Duties of the Department of Technology Planning)

Code of Virginia §2.2-3803
(Administration of systems including personal information; Internet privacy policy)

Executive Order 51 (99)
(Implementing Certain Recommendations by the Governor's Commission on Information Technology)

Scope

This guideline is applicable to all State agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology resources in the Commonwealth. Local government entities are encouraged to review this guidance as well.

Purpose

This guideline is published as a complementary document to the Information Technology Security Standard (i.e., COV ITRM Standard SEC2001-01.1). As such, it contains additional security best practices that are strongly recommended, but which are not required as mandatory. Accordingly, this security guideline should be considered:

1) To further strengthen an agency's information technology security program.
2) To further promote secure communications and the appropriate protection of information resources within the Commonwealth.
3) To further facilitate the alignment and adaptation of security technology to the business needs of the Commonwealth.

General Responsibilities

Secretary of Technology
In accordance with the *Code of Virginia*, the Secretary of Technology, as Chief Information Officer for the Commonwealth, is assigned the following duties: "Direct the formulation and promulgation of policies, standards, specifications and guidelines for information technology in the Commonwealth…"

Council on Technology Services (COTS)
In accordance with the *Code of Virginia*, the Council on Technology Services is assigned the following duties: "establishes COTS to advise and assist the Secretary of Technology in exercising the powers and performing the duties conferred…"

Department of Technology Planning (DTP)
In accordance with the *Code of Virginia*, the Department of Technology Planning is assigned the following duties: "develop and promulgate policies, standards, and guidelines for managing information technology in the Commonwealth".

Department of Information Technology (DIT)
EO-51 (99). D – Directs that "DIT shall develop policies and procedures regarding access to state databases and data communications in order to ensure the security of such databases from unauthorized use, intrusion, or other security threats. DIT shall coordinate the implementation of such policies and procedures with agencies maintaining databases hosted outside of the State Data Center.

All State Agencies
Responsible for complying with COV ITRM policies and standards and considering COV ITRM guidelines issued by the Secretary of Technology.

Definitions

See Glossary

Related COV ITRM Security Policies, Standards, and Guidelines

COV ITRM Policy 90-1: Information Technology Security (Revised 05/19/95)

COV ITRM Standard SEC2001-01.1: Information Technology Security Standard

Table of Contents

Background

This security guideline is published as a complementary document to the Information Technology Security Standard (i.e., COV ITRM Standard SEC2001-01.1). As such, it contains additional security best practices that are strongly recommended, but which are not required as mandatory. Accordingly, this security guideline should be considered:

1) to further strengthen an Agency's information technology security program.
2) to further promote secure communications and the appropriate protection of information resources within the Commonwealth.
3) to further facilitate the alignment and adaptation of security technology to the business needs of the Commonwealth.

COV ITRM Guidelines are directives and specifications, similar to COV ITRM Standards, but advisory in nature only. In essence, guidelines constitute recommendations that are not binding.

As Information Security law, industry standards and technology continue to evolve and mature, the Commonwealth will continue to identify best practices that enable Agencies to further strengthen their security safeguards. However, given the diversity of business processes and platforms in the Commonwealth, it is not always practicable to qualify all security best practices as Commonwealth information technology security standards. Thus, several best practices are more appropriately qualified as "guidelines". Nonetheless, a large percentage of the Commonwealth Agencies will find significant value in formally adopting the best practices listed in this guideline as part of their security programs.

Approach

This COV ITRM Guideline supports the Commonwealth Security Architecture, endorsed by the Council on Technology Services, which consists of the following thirteen security components:

- Business Analysis and Risk Assessment
- Security Awareness
- Technical Training
- Technical Communications
- Authentication, Authorization and Encryption
- Data Security
- Systems Interoperability Security
- Physical Security
- Personnel Security
- Threat Detection
- Security Tool Kit
- Incident Handling
- Monitoring and Controlling System Activities

These components provide a framework that enable secure communications and the appropriate protection of information resources within the Commonwealth. In addition, they provide the

basis for designing the Agency's security program and safeguards. Thus, for each component listed above, a subset of best practices has been identified that, together, comprise this COV ITRM Information Technology Security Guideline.

Detail descriptions of each security component are presented in the Information Technology Security Standard (COV-ITRM SEC2001-01.1) and will not be repeated by this document. Therefore, as this guideline is intended to complement that standard, it is recommended that the Agency become familiar with the contents of said standard in order to better understand this guideline.

Reviews

A full review of the COV ITRM Guideline SEC2001-01.1 is anticipated annually.

Statement of ITRM Best Practices for Information Technology Security

This section groups the best practices of the Information Technology Security Guideline by the thirteen security components that comprise the Commonwealth's Security Architecture.

A. Business Analysis and Risk Assessment

Business Analysis and Risk Assessment refer to those practices, technologies and/or services used to identify information resources that are confidential and/or critical to the Agency; and to identify and evaluate the potential security threats, and associated risks, to those resources.

Best Practices

A.2.a) In assigning the level of risk, each Agency should evaluate both the probability of an event occurring and the resultant effect of that event on the confidentiality, availability, and integrity of system components and data.

B. Security Awareness

Security Awareness refers to those practices, technologies and/or services used to promote User awareness, User training and User responsibility with regards to security risks, vulnerabilities, methods, and procedures related to information technology resources. A "User" is an individual or group who has access to an information system and/or its data.

Best Practices

B.2.a) Security Awareness programs should contain content that covers, but is not limited to:

- Responsibility of users to report issues;
- Users can be audited and monitored;
- Legal requirements for data (citing legislation as appropriate);
- Privacy expectations;
- Ownership of data;
- Acceptable use policy for E-mail and Internet Browsers; and
- Sensitivity to threats, risks, vulnerabilities.

B.2.b) Security Awareness programs should include a means to promote security awareness on an on-going basis, i.e., supplemental to training (e.g., security awareness banners, posters, "security day", etc.)

B.2.c) Security Awareness training content is not static, and should be continuously reviewed and updated by each Agency as needed to reflect changes to the Agency's environment, business, technology, systems and information.

C. Technical Training:

Technical Training refers to those practices, technologies and/or services used in training Security officers, system administrators and/or other personnel involved in the administration or development of information systems.

Best Practices

C.2.a) Each Agency should consider using certification programs to promote high-level, up-to-date technical security expertise (e.g., CISA, CISSP or SANS).

D. Technical Communications:

Technical communications refer to those practices, technologies and/or services used to communicate technical information and notifications regarding the status of security related events and safeguards.

Best Practices

D.2.a) Each Agency should subscribe to industry and vendor security mailing lists for the appropriate system components used within, or interfaced by, the Agency.

D.2.b) Organizations should consider and encourage including information security topics in conferences, symposia, seminars, etc., where appropriate (e.g., Agency Conferences and the Commonwealth of Virginia Information Technology Symposium (COVITS)).

E. Authentication, Authorization and Encryption

Authentication refers to the process of verifying the identity of a user. Authorization refers to the process of establishing and enforcing a user's rights and privileges to access specified resources. Encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

Best Practices:

E.2.a) Each Agency should identify a method of verifying user authenticity on a spectrum from "null/weak" to "strong" authentication methods. Authentication is based on validating the following three criteria presented by the user: 1) "What do you know?", 2) "What do you have?", and 3) "Who are you?". Weak authentication is based on validating one of these criteria only, and should only be used when a minimum level of authentication is desired. Strong authentication, which is based on validating two or more of the criteria, should be used in all other cases.

E.2.b) Each Agency should establish policy and procedures that address when different levels of encryption, digital signatures, and digital certificates are appropriately used.

E.2.c) Digital signature and digital certificate technology can be used by Agencies to verify the authenticity of electronically transmitted data. If high-assurance digital certificates are deemed appropriate, Agencies should use either Virginia On-Line Transaction (VOLT) Certificates, or high-assurance certificates that are compatible with VOLT Certificates.

E.2.d) With regards to Digital Signatures, Agencies should use the VOLT Public Key Infrastructure wherever possible, and should adhere to the Internal Control and Auditing practices established to support the use of digital certificates in the Commonwealth.

E.2.e) Each Agency should identify criteria governing the number of unsuccessful login attempts allowed by a user, and the resetting of passwords.

E.2.f) Authorization should use role-based access models.

E.2.g) Each Agency should use single sign-on technology where appropriate.

E.2.h) Each Agency should strongly consider encryption to protect sensitive data, including passwords, that are transmitted over a public network (e.g., replace Telnet with SSH).

E.2.i) Each Agency should strongly consider encryption to protect sensitive data, including passwords, transmitted over an internal network.

F. Data Security:

Data Security refers to those practices, technologies and/or services used to ensure that security safeguards are applied appropriately to data which is provided, processed, exchanged and/or stored by the State. The term “data” includes, but is not limited to, data in a database, information about an Operating System (OS), operational policies and procedures, system design, organization policies and procedures, system status, and personnel schedules.

Best Practices:

F.2.a) Desktop platforms, including laptops, should have a protected screen saver mechanism, which is activated.

F.2.b) Automatic protected screen savers should be initiated by the system after a specific period of inactivity.

F.2.c) Auditable user agreements should be utilized to delegate responsibility for data security from data owners to data custodians. Custodians are responsible for ensuring that the levels of required protection are followed.

G. Systems Interoperability Security

Systems interoperability refers to those practices, technologies and/or services used to ensure that security safeguards are applied consistently and appropriately to mechanisms that allow diverse systems and networks to interoperate.

Best Practices:

G.2.a) Agencies should use open standard-based security solutions, as opposed to unique generated security solutions, to support current interoperability needs and to position them for future interoperability needs.

G.2.b) Agencies should use open standard based encryption algorithms when sharing sensitive data internally; and externally for data that requires encryption that is resident on that system.

G.2.c) New deployments of VPN (Virtual Private Network) technologies should use IPSec (Internet Protocol Security).

G.2.d) E-mail should not be considered a secure transport in itself. Therefore, any attachment containing sensitive information should be encrypted (e.g., using Pretty Good Privacy (PGP)).

G.2.e) Unencrypted Telnet, FTP, or R-Utilities should not be used.

G.2.f) Secure Shell Protocol (SSH) and Secure Hypertext Transfer Protocol (SHTTP) should be deployed for remote terminal sessions and file transfers.

G.2.g) 40 bit encryption should be used with SSL transactions to ensure global interoperability unless there is a requirement to use a higher bit encryption. (E.g. Virginia Militia or Virginia citizens residing overseas may be limited to 40 bit encryption.)

G.2.h) 1024 bit key digital server certificates should be used for SSL.

G.2.i) Agencies using digital certificates should seek interoperability with those digital certificates utilized by other government bodies(Federal, State, and Local). Virginia On-Line Transaction (VOLT) Certificates are designed for such compatibility.

H. Physical Security

Physical Security refers to those practices, technologies and/or services used to ensure that physical security safeguards are applied. Physical security safeguards take into account 1) the physical facility housing the information resources; 2) the general operating location; and 3) the support facilities that underpin the operation of the information systems.

Best Practices:

H.2.a) Mission critical system components should be located in an environmentally friendly area (e.g., which includes fire protection, HVAC, UPS).

H.2.b) Access to "noncritical" computer hardware, wiring, displays and network should be controlled by rules of least privilege. [Note, see ITRM Security Standard, H.1.b, for access to "critical" components.]

H.2.c) System configurations (i.e., hardware, wiring, displays, network) should be documented. Installations and changes to those physical configurations should be governed by a formal change management process.

H.2.d) Physical Access security for back-up systems should be equivalent to that of the primary facilities.

H.2.e) A system of monitoring and auditing physical access to "noncritical" computer hardware, wiring, displays and networks should be implemented (e.g., badges, cameras, access logs). [Note, see ITRM Security Standard, H.1.d, for monitoring and auditing "critical" components.]

I. Personnel Security

Personnel Security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied appropriately to those personnel working for, or on behalf, of the State.

Best Practices:

I.2.a) Each Agency should establish and document the process which directs the steps and the timing required to grant and withdraw physical and system access privileges to personnel for the following events: new hire, employee transfer to another Agency, employee termination, employee resignation, employee change of job duties within an Agency, and perceived disgruntled employee behavior. A similar process should be established for contractors (i.e., non-state personnel) working for or on behalf of an Agency.

I.2.b) System access should be granted via a formal and auditable process, and should be accompanied by security training which is commensurate to one's duties and responsibilities.

I.2.c) Non-Disclosure Agreements should be signed by all individuals who need access to "sensitive" information, prior to granting access to that information.

I.2.d) Background checks of personnel may be required consistent with Agency policy and depending on the sensitivity of information accessible to that position.

J. Threat Detection

Threat detection refers to those practices, technologies and/or services used 1) to detect that a suspicious activity may be occurring on systems/networks; and 2) to alert security administrators and security staff accordingly.

Best Practices:

J.2.a) Violations of those parameters set in conjunction with the Agency's threat detection program should trigger an appropriate form of security notification to security administrators or security staff.

J.2.b) Systems should be designed to handle both passive and active alarms.

J.2.c) A security event log should be kept for each device. These logs should be analyzed, correlated and evaluated to identify and respond to suspicious activity.

J.2.d) Security logs should be archived on a daily basis.

J.2.e) Security logs should be moved off the device as soon as possible and stored on an off-site location.

J.2.f) Intrusion detection systems should be deployed both externally and internally to the firewall technology protecting the network.

K. Security Tool Kit

This subsection refers to those practices, technologies and/or services used to manage, analyze, filter, test and/or control security safeguards. For example, firewall technology provides a mechanism through which authentication, authorization, filtering and directing of remote users to an internal system can be accommodated. Typically an Agency's security tool kit will be comprised of a combination of commercial off-the shelf products, industry proven free shareware, and Agency developed software tools. The tools may be positioned on the perimeter of systems or integrated into the systems; and may be deployed on either an operational or as needed basis. Examples of common technologies within an organization's security tool kit include firewall technology, vulnerability scanners, and sniffers.

Best Practices:

K.2.a) Within the Agency, firewall technology should be implemented to protect sensitive internal information.

K.2.b) Each Agency should have the ability to monitor and capture traffic at any location within their network (e.g. via use of a portable sniffer).

K.2.c) Each Agency should use network and host vulnerability scanners to test for the vulnerabilities of internal systems and of perimeter defenses, and their adherence to security policy. Resulting vulnerabilities should be addressed.

K.2.d) Each Agency should scan all incoming e-mail for existence of malicious code (e.g., viruses), and contain and eradicate that code.

K.2.e) Each Agency should keep Virus signatures current by updating virus signatures weekly at a minimum.

L. Incident Handling

Incident Handling refers to those practices, technologies and/or services used to respond to suspected or known breaches to security safeguards.

Best Practices:

L.2.a) An Incident Reporting Plan (IRP) should detail the steps to be taken to identify, notify, contain, eradicate, recover from, record and report incidents. (E.g., a reference of a framework for an IRP is available from SANS Institute.)

M. Monitoring and Controlling System Activities

Monitoring and Controlling System Activities refers to those practices, technologies and/or services used to ensure that the implementation and maintenance of security safeguards and system changes are adequately documented and managed, such that accountability can be established.

Best Practices:

M.2.a) System configurations and software change over time. Therefore, each Agency should audit security devices, (e.g., firewalls, routers, secured servers such as E-mail gateways, etc.) on a periodic basis to determine if compliance to security policies is being met.

M.2.b) Each Agency should have a security audit performed by a qualified auditing party external to that Agency on a periodic basis as a supplement to internal auditing activities.

Glossary

Agency – The term "Agency" means executive branch Agencies and institutions of higher education.

Authentication – The term "authentication" refers to the process of verifying the identity of a user.

Authorization – The term "authorization" refers to the process of establishing and enforcing a user's rights and privileges to access specified resources.

CISA – Certified Information Systems Auditor

CISSP – Certified Information Systems Security Professionals

COVITS – Commonwealth of Virginia Information Technology Symposium

Critical (or Mission Critical) – The term "critical" refers to those information resources whose unavailability or improper use has the potential to adversely affect the ability of an Agency to accomplish its mission.

Data – The term "data" includes but is not limited to data in a database, information about an OS, operational policies and procedures, system design, organization policies and procedures, system status, and personnel schedules.

Encryption – The term encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

Firewall Technology – The term "firewall technology" refers any combination of network hardware, network software, and host-based software used within an organization to prevent unauthorized access to system software or data in accordance with its security policy (e.g. includes routers with access list proxy gateways, host-based firewall software, and specialized password devices).

FTP – File Transfer Protocol

HVAC – Heating, Ventilation and Air Conditioning

IETF – Internet Engineering Task Force

Information – The term "information" means any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

Information Resources – The term "information resources" includes government information, information technology and associated personnel.

Information Systems - The term "information systems" means a discrete set of information resources organized for the collection, processing, maintenance, transmission and dissemination of information, in accordance with defined procedures.

Information Technology – The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by an Agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services and related resources.

IPSec – Internet Protocol Security

IRP – Incident Response Plan

ISSO – Information Systems Security Officer (agency-level)

Open Standard – infers that the standard is not proprietary to a specific manufacturer, vendor, product or owner, but may be used among various components and products such that it facilitates interoperability; and it has been approved by an appropriate national or international standards body.

Out-of-band Communication – The term refers to a communication device, platform or media other than that communication media or platform on which a suspected or actual security threat is occurring. Thus, it becomes the alternative communication device, platform or media used to report an incident.

Owner - The term "owner" refers to that group (i.e., Agency or Agency unit) which controls a set of information resources and determines its level of criticality and sensitivity. As such, they determine access, authorization rights, and dissemination regarding those resources.

PGP – Pretty Good Privacy (a security product name)

PKI – Public Key Infrastructure

Policy – The term policy means any general statement of direction and purpose designed to promote the coordinated planning, practical acquisition, effective development, and efficient use of information technology resources.

Public Network – refers to that network infrastructure not controlled by the Agency (e.g., Internet, COVANET).

SANS – Systems Administration, Networking and Security (a cooperative research organization)

Sensitive Information – Sensitive information refers to any confidential or critical information for which the loss, misuse, or unauthorized access to or modification or improper disclosure could adversely affect the Commonwealth's interest, the conduct of Agency programs, or the privacy to which individuals are entitled.

SHTTP – Secure Hypertext Transfer Protocol

SSH – Secure Shell Protocol

SSL – Secure Socket Layer

Standard - The term "standard" means a directive or specification whose compliance is mandatory, and whose implementation is deemed achievable, measurable, and auditable for compliance**.**

TCP/IP – Transmission Control Protocol/Internet Protocol

User – An individual or group who has access to an information system or its data.

VPN – Virtual Private Network

VOLT – Virginia On-line Transaction

Appendix A: Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines

The Department of Technology Planning is responsible for assigning a uniform alphanumeric Publication Designation (PD) to all Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Policies, Standards, and Guidelines (PSG). The PD is derived, in part, from components of the Commonwealth Enterprise Architecture (EA) known as "Infrastructure Domains." The "Infrastructure Domains" and Governance are defined in the Commonwealth EA Glossary. The Governance code is used to identify those PSG that are not uniquely related to a specific infrastructure domain, e.g. "IT Project Management" or "IT Project Oversight."

The following alpha codes will be used to identify each PSG:

Infrastructure Domains + Governance	**Code**
Governance and Transitional Processes	GOV
Platform Architecture	PLA
Database Architecture	DAT
Network Architecture	NET
Security Architecture	SEC
Systems Management Architecture	SYS
Information Architecture	INF
Application Architecture	APP
Middleware Architecture	MID

Publication Designations are constructed as follows:

COV ITRM ("Policy," "Standard," or "Guideline") XXXYYYY-ZZZ

Where: XXX is the assigned Infrastructure Domain + Governance code;
YYYY is the year of initial issue; and
ZZZ is the sequential number assigned to link related PSG.

Example: COV ITRM Standard GOV2000-01.1 is a standard that implements COV ITRM Policy GOV2000-01.1.